UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DIGIPROTECT USA CORPORATION,

Plaintiff,

- against -

JOHN/JANE DOES 1-240,

Defendants.

10 Civ. 8760 (PAC)

OPINION & ORDER

HONORABLE PAUL A. CROTTY, United States District Judge:

On November 19, 2010, DigiProtect USA Corporation ("DigiProtect") commenced this action against 240 Doe Defendants who allegedly infringed its copyright by downloading and distributing unauthorized copies of a pornographic audiovisual work entitled "Let Me Jerk You 2."[1] DigiProtect seeks to identify these unnamed defendants by providing the IP addresses associated with the infringing activity to the corresponding Internet Service Providers ("ISP"). On November 29, 2010 in its Order to Show Cause ("OTSC"), the Court ordered limited discovery to identify the subscribers associated with the IP addresses, "subject to the right of each ISP to challenge this Order upon notice to Plaintiff's counsel prior to the return date of the subpoena" (December 28, 2010). On November 30, 2010, DigiProtect served a subpoena on nine ISPs.

On December 27, 2010, third parties Comcast Cable Communications Management, LLC ("Comcast") and Time Warner Cable, Inc. ("Time Warner"; collectively, "Third Party ISPs") moved (1) to modify the OTSC, and (2) for a protective order. Ninety-six of the Doe Defendants

[1] Patrick Collins, Inc., a California corporation, d/b/a Elegant Angel Productions, a studio located in California, produced the film and claims to hold the copyright. DigiProtect purchased from Patrick Collins, Inc. the limited right to distribute this film via peer-to-peer file sharing networks, such as those allegedly used by the Doe defendants. DigiProtect here exercises this right to bring suit against consumers and seek "modest settlements." DigiProtect USA Corp. v. John/Jane Does 1-266, No. 10 Civ. 8759 (TPG), 2011 WL 1466073, at *1 (S.D.N.Y. Apr. 13, 2011).

are Comcast Internet service subscribers; fifty-five are Time Warner Cable internet service subscribers. The Third Party ISPs argue that complying with the subpoenas would be unduly burdensome in terms of money and time, disrupting their regular business operations and other vital work, such as responding to valid law enforcement requests. They ask the Court to (1) modify the OTSC to "allow for the reimbursement of a substantial amount of the costs Comcast will incur in responding to this or any future subpoena in this action"; and (2) enter a protective order for future subpoenas, limiting the scope of information sought, allowing for a reasonable time to comply, and setting reimbursement amounts. (Mem. in Supp. 1).

At a conference on January 13, 2011, the Court raised the issues of personal jurisdiction over and joinder of the Doe Defendants. After considering the submissions, the Court concludes that DigiProtect failed to establish a *prima facie* case of personal jurisdiction over these 240 unidentified defendants. Publicly available software provides basic, or at least presumptive, geographic information about IP addresses. DigiProtect offers no reason to make the ISPs responsible for locating the defendants within the Court's jurisdiction. Accordingly, the Court vacates the subpoena and dismisses the complaint, with leave to replead naming only John/Jane Doe Defendants over whom there is prima facie personal jurisdiction.

I. Judge Griesa's Decision

On November 19, 2010, the same day DigiProtect filed this action, it also filed in this district a nearly identical complaint, concerning a different pornographic movie, against 266 other Doe Defendants. See DigiProtect USA Corp. v. John/Jane Does 1-266, No. 10 Civ. 8759 (TPG). That case was assigned to U.S. District Judge Thomas P. Griesa, who signed a nearly identical OTSC and subpoena. DigiProtect, 2011 WL 1466073, at *1. The Third Party ISPs moved to modify the OTSC and for a protective order. Judge Griesa held a hearing on February

2, 2011, at which he ordered Comcast and Time Warner to inform the court of the IP addresses connected to internet accounts located in New York State. Id. The Court learned that, of the 103 IP addresses corresponding to Comcast accounts, none were located within New York State; and, of the 43 IP addresses corresponding to Time Warner accounts, only ten were located within New York State. Id. at *2. At a subsequent telephone conference, DigiProtect informed the court that, based on its own research, only twenty to twenty-five of all 266 Doe Defendants used internet accounts located in New York State. Id. at *2. On April 13, 2011, Judge Griesa granted the motions, limiting discovery to ISP accounts located in New York State. Id. at *5.

II. Discussion

A. Personal Jurisdiction

DigiProtect argues that the Court has personal jurisdiction over the unnamed defendants because DigiProtect, as the copyright license-holder, suffered injury in New York, and because the nature of peer-to-peer file sharing networks connects all out-of-state defendants with defendants residing in New York. (Mem. in Supp. 4-5).

The Court may deny discovery if the plaintiff cannot make a prima face case for personal jurisdiction over a defendant. See, e.g., Best Van Lines, Inc. v. Walker, 490 F.3d 239, 255 (2d Cir. 2007). The Court applies the law of the forum state—New York—on personal jurisdiction. Fort Knox Music Inc. v. Baptiste, 203 F.3d 193, 196 (2d Cir. 2000). General jurisdiction requires that the defendant reside, do business, or be served with process while in New York. See N.Y. C.P.L.R. § 301; see, e.g., Landoil Res. Corp. v. Alexander & Alexander Servs., Inc., 565 N.E.2d 488, 490 (N.Y. 1990).

New York's long arm statute also provides jurisdiction over nondomiciliaries who commit a tortious act within the state, N.Y. C.P.L.R. § 302(a)(2); or a tortious act outside the

state that resulted in injury within New York, id. § 302(a)(3)(ii). For a copyright infringement claim, under § 302(a)(2), the tortious act committed within the state is the act of infringement, or the illegal download. Yash Raj Films (USA) Inc. v. Dishant.com LLC, No. 08-CV-2715 (ENV)(RML), 2009 WL 4891764, at *7 (E.D.N.Y. Dec. 15, 2009). Under § 302(a)(3)(ii), only the injury must occur in New York; the act of downloading may occur outside the state, but the plaintiff must also show that the nondomiciliary "expects or should reasonably expect the act to have consequences in the state and derives substantial revenue from interstate or international commerce." N.Y. C.P.L.R. § 302(a)(3)(ii).

Finally, the Due Process Clause requires proof that out-of-state defendants have "certain minimum contacts . . . such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." Calder v. Jones, 465 U.S. 783, 788 (1984) (quotations omitted).

The New York Court of Appeals recently held that, while the site of injury under § 302(a)(3)(ii) in commercial tort cases traditionally has been where business is lost, rather than where the plaintiff is located, "the unique bundle of rights granted to copyright owners" "tips the balance in favor of New York as the situs of the injury" when a New York company's copyright is infringed by unauthorized publishing on the internet. Penguin Grp. (USA) Inc. v. Am. Buddha, 946 N.E.2d 159, 176 (N.Y. 2011).

At this point, the Court need not decide whether the Court of Appeals' reasoning extends to a New York company, DigiProtect, that holds a limited right, while an out-of-state California company, Patrick Collins Inc., retains most of the bundle of rights as copyright holder. Even assuming the alleged injury is in New York, DigiProtect has failed to satisfy the other requirements of long-arm jurisdiction. There is no evidence "that any of the Doe Defendants expected or reasonably should have expected their downloading of this film to have

consequences in New York, particularly when the producer of the film is located in California." DigiProtect, 2011 WL 1466073, at *4. Likewise, there is no basis to allege that the unnamed defendants derived substantial revenue from interstate or international commerce. See id. Accordingly, DigiProtect has not made a *prima facie* showing of long-arm jurisdiction over out-of-state defendants.

The Court rejects DigiProtect's argument that it has personal jurisdiction as to all 240 defendants, if any one resides in New York. Its argument is based on the nature of peer-to-peer networks in which unauthorized copies are distributed among peers.[2] The mere fact that BitTorrent protocol and eDonkey network employ "swarming" capacity is insufficient to confer jurisdiction. DigiProtect does not allege that John/Jane Does served as each others' agents or conspired together, as required under § 302(a)(2), Lehigh Valley Indus., Inc. v. Birenbaum, 527 F.2d 87, 93-94 (2d Cir. 1975); or purposely availed themselves of New York, as required by the Due Process Clause, Hanson v. Denckla, 357 U.S. 235, 253 (1958). (See Compl. ¶ 10). Indeed, DigiProtect states that copies produced by swarming are unauthorized. (Id. ¶ 11). While this technology may make it possible for two strangers to enable each other to commit infringement without even knowing it, this mere possibility does not suggest that it has actually occurred; they may have participated in entirely different swarms. Pac. Century, 2011 WL 2690142, at *3

[2] This technology functions as follows:

> First, the protocol breaks a single large file into a series of smaller distributable pieces. Then, an initial file-provider (the "seeder") intentionally elects to distribute the pieces to third parties. . . . Other users ("peers") on the network download a small "torrent" file that contains directions on where to find the seeder as well as an index of the pieces. The torrent file is loaded into BitTorrent software, and the software follows the directions in the torrent file to connect to the seeder. When peers connect to the seeder, they download random pieces of the file being seeded. When a piece of download is complete, the peers automatically become seeders with respect to the downloaded pieces. In other words, each peer in a swarm transforms from a pure downloader . . . to a peer that is simultaneously downloading and distributing pieces of a file.

Pac. Century Intern. Ltd. v. Does 1-101, No. C–11–02533–(DMR), 2011 WL 2690142, at *3 (N.D. Cal. July 08, 2011). To participate, a user must be online at the time of a swarm. Donkeyball Movie, LLC v. Does, No. 10–1520 (BAH), 2011 WL 1807452, at *5 (D.D.C. May 12, 2011).

("Plaintiff glosses over the fact that BitTorrent users may upload different initial files of a given work, which results in the creation of distinct swarms . . . , [and] the participants in the first swarm would not interact with those in the second swarm. That BitTorrent users have downloaded the same copyrighted work does not, therefore, evidence that they have acted together to obtain it." (internal citations omitted)). For example, the Complaint does not allege that any of the 240 John/Jane Does downloaded the movie from the same website during overlapping times. Id. (noting that swarming is only possible "until the user manually disconnects from the swarm or the BitTorrent client otherwise does the same"). Nor does it present any information about a suspected infringer's ability to refrain from participating in swarming conduct.[3] Absent intentional conduct, there can be no personal jurisdiction.

Comcasts reports that "none of the IP addresses designated as a Comcast IP address in [this action] is for a subscriber in New York State." Letter from Comcast, Feb. 14, 2011, at 1. Like Judge Griesa, the Court does not want to "ensnar[e] unsophisticated individuals from around the country in a lawsuit based in New York," who likely would be encouraged to settle rather than incur the burden and embarrassment of contesting the litigation. DigiProtect, 2011 WL 1466073, at *2. Since it has failed to make a *prima facie* showing of long arm jurisdiction under § 302(a)(3)(ii), DigiProtect is only permitted to proceed against those defendants

[3] For the same reasons, DigiProtect cannot join hundreds of individuals in a single case by alleging that they infringed the same copyright by illegally downloading the same movie, albeit in separate instances. The swarming capacity of peer-to-peer networks alone does not mean that John/Jane Does actually engaged in "the same transaction, occurrence, or series of transactions or occurrences," as required by Fed. R. Civ. P. 20(a)(2)(A). See Pac. Century, 2011 WL 2690142, at *3 (finding allegation that defendants downloaded same work, without evidence that they participated in the same swarm, insufficient); W. Coast Prods., Inc. v. Does 1-5829, No. 11-57 (CKK), 2011 WL 2292239, at *5 (D.D.C. June 10, 2011) (finding joinder appropriate because the complaint alleged that all unidentified defendants participated in a single swarm); Patrick Collins, Inc. v. Does 1-118, No. 3:10-CV-92, slip op. at 2-3 (N.D.W. Va. Dec. 16, 2010). But see, e.g., Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332, 343 (D.D.C. 2011). Any repleading by DigiProtect must be based on specific factual allegations connecting these defendants to the same specific swarming transaction, or series of transactions, to support their joinder. Otherwise, the only "commonality" is that "each commit[ted] the exact same violation of the law in exactly the same way." Pac. Century, 2011 WL 2690142, at *4 (internal quotations omitted). The current allegations are inadequate to support joinder.

otherwise subject to personal jurisdiction in New York (e.g., who reside in New York or illegally downloaded the movie while physically in New York). A showing that the internet account associated with an IP address that allegedly engaged in infringing activity is located in New York State is sufficient to establish prima facie personal jurisdiction over the alleged infringer. See also CP Prods., Inc. v. Does 1-300, No. 10 C 6255, 2011 WL 737761, at *1 (N.D. Ill. 2011) ("[T]here is no justification for dragging into an Illinois federal court, on a wholesale basis, a host of unnamed defendants over whom personal jurisdiction clearly does not exist and-more importantly-as to whom [plaintiff's] counsel could readily have ascertained that fact.").

Information about the geographic location of internet accounts connected to specific IP addresses "is easily accessible and publicly available." DigiProtect, 2011 WL 1466073, at *2; see also Letter from Comcast, Feb. 14, 2011, at 1 (reporting its results, "initially made using a free, publicly-available website that matches an IP address with the Internet service provider to which it's assigned and lists the geographic region in which the provider uses the address,[which] could easily have been done by Plaintiff at the outset"). While the Court may allow discovery to determine the basis for personal jurisdiction, Sony Music Entm't Inc. v. John Does 1-140, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004), DigiProtect offers no reason why it should be excused from making a *prima facie* showing that the Defendants are connected to New York, particularly when this information is publicly available. Rather, it asks the Court to order the Third Party ISPs to bear this burden. Accordingly, the Complaint is dismissed, with leave to replead, naming only those John/Jane Does as to whom there is *prima facie* personal jurisdiction.

B. Cost of Compliance

Third-Party ISPs also seek protective orders requiring DigiProtect to reimburse them for the costs of complying with the subpoenas. They argue that "[t]he process for linking IP

addresses to subscriber account details such as name and address [a 'look-up'] is time consuming and requires careful, systematic processes to ensure the integrity and accuracy of the results." Additionally, federal law required cable operators such as Comcast to give notice to any subscriber whose identity is sought before any disclosure is made, to allow the subscriber to take preventative measures. Comcast estimates the "pure cost" associated with each IP address look-up at approximately $120 ($95 for administrative processing; $25 for overnight mail notification). This total includes running look-ups through two systems; labor to confirm authenticity and accuracy; notification by overnight mail; copying the OTSC and subpoena; and interacting with responding subscribers or their attorneys. Finally, Comcast asserts that it processes approximately 200 court orders, subpoenas, and warrants requesting subscriber identification per business day; and that it must prioritize emergency and law enforcement requests. (Mem. in Supp. 5).

DigiProtect does not contest these facts. It argues, instead, that the Digital Millenium Copyright Act ("DCMA"), 17 U.S.C. § 512 requires the ISPs to provide this information anyway. (Mem. in Opp. 10-11).[4] This argument is wrong. See DigiProtect, No. 10 Civ. 8759 (TPG), Dkt. 22 (May 23, 2011 Order).

In deciding on how to next proceed, Plaintiff should recognize that its approach imposes a substantial burden on parties with no formal interest in the outcome of the litigation. Fed. R. Civ. P. 26(b)(2)(C) requires the court to enter a protective order limiting discovery where "the burden or expense of the proposed discovery outweighs its likely benefit." Courts are especially sensitive to the burdens placed on nonparties. See Cusumano v. Microsoft Corp., 162 F.3d 708, 717 (1st Cir. 1998); Dart Indus. Co. v. Westwood Chem. Co., 649 F.2d 646, 649 (9th Cir. 1980).

[4] DigiProtect also relies on this argument, set forth in its April 7, 2011 letter and subsequent submissions, in requesting leave to serve a supplemental subpoena on Comcast and Time Warner. The Court denies this request for the same reasons.

Accordingly, the Court will require DigiProtect to reimburse the ISPs for the costs incurred in each IP address look-up, including notifying the relevant subscribers. Nor are the ISPs at the beck and call of DigiProtect. The ISPs may limit the requests to no more than 25 IP address look-up requests per month. The ISPs will have thirty days from the date of notice to the subscriber to provide a response for each set of twenty-five IP addresses. The cost allowances and limitations on look-ups are based on a per IP address, rather than per subscriber, basis.

III. Conclusion

Accordingly, the Court vacates the subpoena and dismisses the complaint with leave to replead, within 30 days of this decision. The Clerk of the Court is directed to close this case.

Dated: New York, New York
September 26, 2011

SO ORDERED

PAUL A. CROTTY
United States District Judge